



United States
Department of
Agriculture

Farm Service Agency
ADC/AFAO/AGG
6501 Beacon Drive
Kansas City, MO 64133-4676

Privacy Impact Assessment (PIA)

GSM Export Credit Guarantee Systems (GSM/Web/PC)

Date: September 03, 2008



Revision: Final



Document Information

Owner Details	
Name	Ethel Anderson, CSO
Contact Number	(816)926-1923
E-mail Address	Ethel.anderson@kcc.usda.gov

Document Revision and History			
Revision	Date	Author	Comments
	07/01/2008	C. Caruthers, AFAO-AGG	Updated for SQL Server Database Implementation
Draft V.1	08/15/2008	S.Timbrook, ECS	Changed layout to new template, reviewed for updates. Changed System description to only reflect GSM/Web/PC.
Draft V.1	08/19/2008	C. Caruthers, AFAO-AGG	Updated new template document.
Draft V.2	08/20/2008	S. Timbrook, ECS	Reviewed and added Completed by, returned for clarification of questions.
Draft V.2.o	8/20/2008	C. Caruthers, AFAO-AGG	Updated system overview and completed Privacy Impact Assessment.
Final	08/25/2008	R. Grant-Smith, ECS	Marked document as final and forwarded to Karen A. Malkin, Esq., for review and signature.
Final	8/25/2008	S. Timbrook, ECS	Reviewed Document, Marked Final, Updated to reflect new Acting CIO Sue Bussels and changed Information System Owner to Angela Sieg, Sent out for Signatures
Final	09/03/2008	S. Timbrook, ECS	Marked Final and change date to reflect current date 09/03/2008. Corrected Karen Malkin's Title through out the document to reflect "Esq. Chief Privacy Officer and Assistant to the Administrator", Replaced Karen Malkin, Esq. with Brain Davies ISSPM on signatures page.



Table of Contents

1	PURPOSE OF DOCUMENT	1
2	APPLICABILITY	2
	Applicability of System	2
	System Overview	2
	System Categorization	2
	Responsible Organization	2
	Information Contacts.....	3
	Assignment of Security Responsibility.....	4
2.1	Who Completed this Assessment?	4
3	USDA PRIVACY IMPACT ASSESSMENT.....	5
3.1.1	Data Collection.....	7
3.1.2	Data Use	8
3.1.3	Data Retention.....	9
3.1.4	Data Sharing.....	10
3.1.5	Data Access.....	11
3.1.6	Customer Protection.....	12
3.1.7	System Of Record	13
3.1.8	Technology.....	13
4	PRIVACY IMPACT ASSESSMENT AUTHORIZATION MEMORANDUM.....	17



1 Purpose of Document

USDA DM 3515-002 states: "Agencies are responsible for initiating the PIA in the early stages of the development of a system and to ensure that the PIA is completed as part of the required System Life Cycle (SLC) reviews. Systems include data from applications housed on mainframes, personal computers, and applications developed for the Web and agency databases. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in USDA.

Both the system owners and system developers must work together to complete the PIA. System owners must address what data are used, how the data are used, and who will use the data. System owners also need to address the privacy implications that result from the use of new technologies (e.g., caller identification). The system developers must address whether the implementation of the owner's requirements presents any threats to privacy."

The Privacy Impact Assessment (PIA) document contains information on how the GSM Export Credit Guarantee System (GSM/Web/PC) affects the privacy of its users and the information stored within. This assessment is in accordance with NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*.



2 Applicability

Applicability of System

The information in this document is applicable to the General Sales Manager Export Credit Guarantee System (GSM Web/PC).

System Overview

The General Sales Manager Export Credit Guarantee System (GSM Web/PC) is an application-based system that supports both the USDA Farm Service Agency (FSA) and the Foreign Agricultural Service (FAS). The application's mission is to provide reporting of financial and GSM-102 program data to the FSA Financial Management Division (FMD) via the General Sales Manager Data Mart (GSMDM) and to provide application operational support for FAS.

The GSM Web/PC application is used to gather structured and unstructured financial data and prepare this information to be streamlined within the GSMDM. The application follows a distributed architecture where the Web interface resides in the Web Farm, the PC application client resides on a networked drive, and the database server (SQL Server 2000) resides on the VMWare ESX - Virtual Server. The application employs Secure File Transfer Protocol (SFTP) to connect to the Informix data mart server at OCIO-NITC to retrieve financial information from the GSM database server (SQL Server 2000). The GSM Web/PC application also transfers accounting data for the Core Accounting System from the IMPD2 fileservers to the mainframe.

System Categorization

By following the guidance set forth in NIST SP 800-60 and FIPS PUB 199 taking into account the information types and other factors for this system, the Security Categorization for this system has been determined to be Moderate. Therefore, Risk Assessments and Security Testing and Evaluation (ST&E) will be performed following the **Moderate** baseline set forth in NIST SP 800-53 Annex 2.

Responsible Organization

United States Department of Agriculture (USDA)
Farm Service Agency (FSA)
1400 Independence Avenue SW
Washington, D.C. 20250

This system is maintained by:

Farm Service Agency
Farm Service Agency
Administrative & Financial Applications Office/AGG Group
6501 Beacon Drive



Kansas City, MO 64133

This system's hardware is located at:

OCIO/ITS
GSM Sales Manager Export Credit Guarantee System (Web/PC)
8930 Ward Parkway
Kansas City, MO 64114

Information Contacts

Name	Title	Address	Phone Number	E-mail Address
Certifying Officer: Sue Bussells	FSA Chief Information Officer Director, Information Technology Services Division (ITSD) FSA/DAM/ITSD	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington D.C. 20250	(202)720-5320	sue.bussells@wdc.usda.gov
Business Owner (DAA): Dennis Taitano	Director, FSA/DAM/BUD and Director, FSA/DAM/FMD	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington D.C. 20250	202-720-3674	dennis.taitano@wdc.usda.gov
Business Program Manager: Agnes Leung	Director, International and Treasury Operations Center (ITOC) FSA/DAM/FMD/ITOC	U.S. Department of Agriculture Farm Service Agency	703-305-1380	agnes.leung@wdc.usda.gov
System Owner: Ethel Anderson	AFAO, Office Chief	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-1923	ethel.anderson@kcc.usda.gov
System Manager: Angela Sieg	Group Chief, Administrative & Financial Applications Office/AGG Group	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-9261923	angela.sieg@kcc.usda.gov I



Assignment of Security Responsibility

Name	Title	Address	Phone Number	E-mail Address
Karen Malkin , Esq.	Chief Privacy Act Officer and Assistant to the Administrator USDA/FSA/OA/OBPI/SPS	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-690-2203	karen.malkin@wdc.usda.gov
Thomas B. Hofeller,	Freedom of Information Act (FOIA) Coordinator Associate Administrator for Operations and Management USDA/FSA/OA	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-690-0153	tom.hofeller@wdc.usda.gov
Brian Davies	Information System Security Program Manager (ISSPM) FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-720-2419	brian.davies@wdc.usda.gov
Mindy Gehrt	Disaster Recovery Coordinator Information Security Office (ISO) FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-3522	mindy.gehrt@kcc.usda.gov
Georgia "Shelly" Nuessle	Certification & Accreditation Coordinator Information Security Office (ISO) USDA - FSA/DAM/ITSD/OTC/ISO	U.S. Department of Agriculture Farm Service Agency 6501 Beacon Drive Kansas City, MO 64133	816-926-3018	georgia.nuessle@kcc.usda.gov

2.1 Who Completed this Assessment?

August 19, 2008
Chris Caruthers, AFAO-AGG
IT Specialist
6501 Beacon Drive
Kansas City, MO 64133
816-926-6848
Chris.caruthers@kcc.usda.gov



3 USDA Privacy Impact Assessment

QUESTION 1 Does the system contain any of the following type of data as it relates to individuals:	Yes		No
	Citizens	Employees	
Name	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Social Security Number	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Telephone Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Email address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Street address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Financial data	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Health data	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Biometric data	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code ¹	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Are social security numbers embedded in any field?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Is any portion of a social security numbers used?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>



If all of the answers in Questions 1 and 2 are NO,

You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets,

Part 7, Section E, Question 8c is:

¹ Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.



3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.



3.1.1 Data Collection

1. Generally describe the data to be used in the system.

Customer data: evidence of export, notice of default, notice of assignment, claims, recoveries, fees, guarantee bank name, payment bank name and payment bank account number.

2. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

- ☒ Yes
☐ No

3. Sources of the data in the system.

- 3.1. What data is being collected from the customer?

Customer data: evidence of export, notice of default, notice of assignment, claims, recoveries, fees, guarantee bank name, payment bank name and payment bank account number.

- 3.2. What USDA agencies are providing data for use in the system?

Foreign Agricultural Service (FAS), Farm Service Agency (FSA) Financial Management Division

- 3.3. What state and local agencies are providing data for use in the system?

None Applicable

- 3.4. From what other third party sources is data being collected?

U.S. Treasury Department

4. Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

- ☒ Yes
☐ No. If NO, go to section 3.1.2, question 1.

- 4.1. How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?

Reconciliation and Review by Farm Service Agency (FSA) – Financial Management Division



(FMD)

- 4.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

Reconciliation and Review by Farm Service Agency (FSA) – Financial Management Division (FMD)

3.1.2 Data Use

- 1 Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?

Per GSM-102/103 program law, the Commodity Credit Corporation (CCC) directs the administration of the GSM system.

- 2 Will the data be used for any other purpose?

☐ Yes
☒ No. If NO, go to question 3 (below).

2.1 What are the other purposes?

- 3 Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

☒ Yes
☐ No

- 4 Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

☐ Yes
☒ No. If NO, go to question 5 (below).

4.1 Will the new data be placed in the individual's record (customer or employee)?

☐ Yes
☐ No

- 4.2 Can the system make determinations about customers or employees that would not be possible without the new data?



- ☐ Yes
☐ No

4.3 How will the new data be verified for relevance and accuracy?

- 5 Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?

This data is used to administer the GSM program.

- 6 Will the data be used for any other uses (routine or otherwise)?

- ☐ Yes
☒ No. If NO, go to question 7 (below).

6.1 What are the other uses?

- 7 Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

- ☐ Yes
☒ No. If NO, go to question 8 (below).

7.1 What controls are in place to protect the data and prevent unauthorized access?

- 8 Are processes being consolidated?

- ☐ Yes
☒ No. If NO, go to section 3.1.3, question 1.

8.1 What controls are in place to protect the data and prevent unauthorized access?

3.1.3 Data Retention

- 1 Is the data periodically purged from the system?
Data is not purged from the GSM System.

- ☐ Yes
☒ No. If NO, go to question 2 (below).



- 1.1 How long is the data retained whether it is on paper, electronically, in the system or in a backup?
- 1.2 What are the procedures for purging the data at the end of the retention period?
- 1.3 Where are these procedures documented?
- 2 While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Reconciliation and Review

- 3 Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

- ☒ Yes
☐ No

3.1.4 Data Sharing

- 1 Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

- ☒ Yes
☐ No. If NO, go to question 2 (below).

- 1.1 How will the data be used by the other agency?

The data will be used by the Office of Foreign Assets Control ("OFAC") of the U.S. Treasury Department. The OFAC office ensures that terrorist, international narcotics traffickers and other restricted persons are not allowed to participate in U.S. Government programs such as GSM.

- 1.2 Who is responsible for assuring the other agency properly uses of the data?

The data recipient is responsible for the proper use of the data. All data that is forwarded contains the following statement. This e-mail and any attachments may contain sensitive data. It is your responsibility to adhere to USDA policies and notices in the internal and external use and protection of sensitive data. If you authorize the release of this information you must ensure the recipient is notified that the data is sensitive and that the recipient is responsible for securing and protecting the data.



2 Is the data transmitted to another agency or an independent site?

- ☐ Yes
☒ No. If NO, go to question 3 (below).

2.1 Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

3 Is the system operated in more than one site? Where?

- ☒ Yes
☐ No. If NO, go to section 3.1.5, question 1.

3.1 How will consistent use of the system and data be maintained in all sites?

Reconciliation and Review

3.1.5 Data Access

1 Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

Customers, USDA employees have Update Access, Exporters may submit data online and by request through FSA or FSA, OIG and Congress may receive reports.

2 How will user access to the data be determined?

The users access to data is based upon his/her submitted FSA-13a data access form.

2.1 Are criteria, procedures, controls, and responsibilities regarding user access documented?

- ☒ Yes
☐ No

3 How will user access to the data be restricted?

An employee's system access is based upon his/her job duties.

3.1 Are procedures in place to detect or deter browsing or unauthorized user access?

- ☒ Yes
☐ No

4 Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?



- ☒ Yes, the GSM system employs e-authentication and application role-based security.
☐ No

3.1.6 Customer Protection

- 1 Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e. office, person, departmental position, etc.)?

Farm Service Agency (FSA) – Financial Management Division (FMD).

- 2 How can customers and employees contact the office or person responsible for protecting their privacy rights?

Customers can contact the USDA/FSA Privacy Officer at the following address:

Name	Address	Phone Number	E-mail Address
Chief Privacy Officer and Assistant to the Administrator: Karen Malkin, ESQ	U.S. Department of Agriculture Farm Service Agency 1400 Independence Avenue SW Washington, D.C. 20250	202-690-2203	karen.malkin@wdc.usda.gov

- 3 A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

- ☒ Yes. If YES, go to question 4 (below).
☐ No

3.1 If NO, please enter the POAM number with the estimated completion date:

- 4 Consider the following:
- Consolidation and linkage of files and systems
 - Derivation of data
 - Accelerated information processing and decision making
 - Use of new technologies

Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?

- ☐ Yes
☒ No. If NO, go to question 5 (below).

4.1 Explain how this will be mitigated?

- 5 How will the system and its use ensure equitable treatment of customers?



- 6 Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?

☐ Yes
☒ No. If NO, go to section 3.1.7, question 1.

6.1 Explain

3.1.7 System Of Record

- 1 Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

☐ Yes
☒ No. If NO, go to section 3.1.8, question 1.

1.1 How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

1.2 Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. The SORS for FSA can be viewed at <http://www.gpoaccess.gov/privacyact/index.html>. Copy the following search element, including quotes, into the search box: "USDA/FSA-"

1.3 If the system is being modified, will the SOR require amendment or revision?

3.1.8 Technology

- 1 Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

☐ Yes
☒ No. If NO, the Questionnaire is Complete.

1.1 How does the use of this technology affect customer privacy?

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:



1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION
OFFICE/CYBER SECURITY



Privacy Impact Assessment for
GSM Export Credit Guarantee System (GSM/Web/PC)



Privacy Impact Assessment for
GSM Export Credit Guarantee System (GSM/Web/PC)

4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

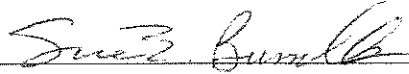
GSM Export Credit Guarantee System (GSM/Web/PC)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed.
Based on our authority and judgment, the continued operation of this system is authorized.

Stephen Risker
System Manager/Owner

Date



Sue Bussells
Agency CIO



Date

Karen Malkin
Chief Privacy Act Officer

Date



Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

GSM Export Credit Guarantee System (GSM/Web/Pc)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed.
Based on our authority and judgment, the continued operation of this system is authorized.

Angela Sieg
System Manager/Owner

Date

Sue Bussells
Agency CIO (Acting)

Date

Brian Davies

9/9/2008

Brian Davies
Information System Security Program Manager (ISSPM)

Date



4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

GSM Export Credit Guarantee System (GSM/Web/Pc)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed.
Based on our authority and judgment, the continued operation of this system is authorized.

Angela Sieg
System Manager/Owner

Date

Sue Bussells
Agency CIO (Acting)

Date

Brian Davies
Information System Security Program Manager (ISSPM)

Date